PRE-APPEAL BRIEF REQUEST FOR REVIEW		**Docket Number:** TUC920010022US1
I hereby certify that this correspondence is being transmitted via the EFS-Web System to the USPTO on: July 24, 2008 Signature: /David Victor/ Typed or Printed Name: David W. Victor	**Application Number:** 09/977,159	**Filed:** October 11, 2001
	First Named Inventor: G.A. JAQUETTE	
	Art Unit: 3621	**Examiner:** Firmin Backer

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached five (5) sheet(s).
Note: No more than five (5) pages may be provided.

I am the:

☐ applicant/inventor	/David Victor/ Signature
☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)	David W. Victor Typed or Printed Name
☒ attorney or agent of record. Registration Number Registration No. 39,867	(310) 553-7977 Telephone Number
☐ attorney or agent acting under 37 CFR 1.34 Registration number if acting under 37 CFR 1.34 ________________	July 24, 2008 Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required*.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	G.A. JAQUETTE	Examiner	Firmin Backer
Serial No.	09/977,159	Group Art Unit	3621
Filed	October 11, 2001	Docket No.	TUC920010022US1
TITLE	METHOD, SYSTEM, AND PROGRAM FOR SECURELY PROVIDING KEYS TO ENCODE AND DECODE DATA IN A STORAGE CARTRIDGE		

PRE-APPEAL BRIEF REQUEST FOR REVIEW ARGUMENTS

Applicants request review of the rejection of claims 1-17 as obvious (35 U.S.C. §103(a)) over Shear (U.S. Patent Pub. 2001/0042043) and O'Connor (U.S. Patent No. 5,745,568) in the Final Office Action dated March 24, 2008 ("FOA)".

With respect to claim 1, Applicants request review of the Examiner's finding that col. 4, lines 2-16 of O'Connor teaches the claim requirements of receiving, by the interface devices, an Input/Output (I/O) request; decrypting, by the interface devices, the encrypted coding key in response to the I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the at least one storage cartridges to perform the received I/O request. (FOA, pgs. 2-3)

The cited col. 4 of O'Connor discusses a technique to install a program from a CD-ROM onto a computer system. The CD-ROM program runs a hardware identifier routine that retrieves the hardware identifier associated with a customer's computer system. A verify software hardware step reads the hardware identifier written to a loaded CD ROM, compares the hardware identifier of the computer and the CD-ROM. If they match, a routine decrypts the software files using the hardware identifier as a decryption keys. The decrypted files are then installed. Further, the hardware identifier may also be used as a decryption key.

Nowhere does the cited col. 4 of O'Connor teach or suggest the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the target storage cartridge to perform the received I/O request. For instance, nowhere does the cited O'Connor mention decrypting the hardware identifier, which O'Connor mentions is used to decrypt files. Instead, the cited O'Connor discusses decrypting files if identifiers match and then installing the decrypted files. There is no teaching or mention of the claim requirement of decrypting a key for an I/O request to code data to be written to perform the I/O request.

Moreover, Applicants further submit that O'Connor teaches away from the claim requirement that multiple interface devices decrypt the encrypted coding key to use to code data to write to the storage cartridges. O'Connor mentions the use of a hardware identifier specific to hardware to decrypt data and verify the operation. Consequentially, O'Connor teaches away from different interface devices using the same encrypted coding key because in O'Connor each devices unique hardware identifier is used to decrypt and verify operations. Further, O'Connor does not teach or suggest using an encrypted coding key to code data as claimed.

Applicants further submit that both O'Connor and Shear are deficient because the concern techniques to decrypt data. Nowhere do these references alone or in combination teach or suggest the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to code data to be written to perform the received I/O request. Further, nowhere is there any teaching that multiple interface devices decrypt the encrypted coding key to use to code data to write to the storage cartridges.

With respect to claim 8, Applicants request review of the Examiner's finding that FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the claim requirements that encrypting the coding key further comprises: encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key; encrypting the second key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device. (FOA, pgs. 4-5)

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recorded. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable. The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted. The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties. The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media. The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches encrypting the key used to decrypt the coding key with a third key, and that the interface device, or cited drive, uses a fourth key to decrypt the coding key, or cited encrypted key block. Further, the Examiner has not cited any part of Shear that teaches transmitting the decryption key encrypted with a first key and the second key encrypted with a third key to the interface device. In other words, the Examiner has not cited any part of Shear that teaches encrypting the key used to decrypt the coding key.

With respect to claim 9, Applicants request review of the Examiner's finding that the above cited Shear teaches the claim requirements that encrypting the coding key comprises: encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key; transmitting the coding key encrypted with the first key to the interface device; receiving, from the interface device, the coding key encrypted with the first key; decrypting the coding key with the second key; encrypting the coding key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the third key to the interface device. (FOA, p. 5)

The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. Although the cited Sheer discusses encrypting a decrypting key used to decrypt content on the disk with on or more keys, the Examiner has not cited any part of Shear that teaches receiving the coding key encrypted with a first key from the interface device, decrypting the coding key with a second key, reencrypting the coding key with a third key and transmitting that reencrypted coding key to the interface device, which uses a fourth key to decrypt. For instance, the Examiner has not cited any part of Shear that teaches that the DVD drive transmits the encrypted coding key to another device that decrypts that key and reencrypts with a key with a yet further key that the drive can decrypt.

With respect to independent claim 10, Applicants request review of the Examiner's finding that the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teaches the claim requirements. (FOA, pg. 5)

The cited Shear does not teach the claim requirements of an interface device for accessing a coupled storage medium receive an encrypted key from a host with an I/O request to decrypt and use to encode data to write to the storage medium for a write I/O request and decode data read from the storage for a read I/O request. Instead, as discussed, the cited Shear discusses a drive accessing an encrypted decrypting key to use to decrypt content on a disk (DVD), not decrypting the decrypted encoding key to use encode data to write to the storage medium for an I/O request as claimed.

Further, the Examiner has not cited any part of the references that teaches the claim requirement of storing the received encrypted coding key in the storage medium to use for subsequent I/O requests. The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. However, these cited sections do not teach that the disk drive, which decrypted and used a key to code data to write to the storage, stores the received encrypted coding key in the storage medium for subsequent I/O requests.

With respect to claim 16, Applicants request review of the Examiner's finding that the above discussed Shear teaches the claim requirements. (FOA, pgs. 6-7)

The cited Shear does not teach that the coding key, corresponding to the cited decryption key, is encrypted with a first key and that the interface device receives a second key encrypted with a third key that it decrypts with a fourth key to then use the second key to decrypt encrypted coding key to use. For instance, the Examiner has not cited where Shear teaches that the disk drive receives a further key that is used to decrypt the key it maintains to use to decrypt the key block on the DVD. Instead, the cited Shear, including para. 0217, mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Dated: July 24, 2008

By: /David Victor/
David W. Victor
Registration No. 39,867
Tel: (310) 553-7977